BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646)-837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

Attorney for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MATTHEW MILLER, individually and on behalf of all other persons similarly situated,

Plaintiff,

vs.

NEWPORT HARBOR PATHOLOGY GROUP, INC. d/b/a ORANGE COUNTY MEDICAL GROUP PATHOLOGY d/b/a/ MISSION LAGUNA PATHOLOGY MEDICAL GROUP d/b/a BARR DERMATOPATHOLOGY,

Defendant.

Case No. 8:25-cv-704

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Matthew Miller ("Plaintiff") files this class action complaint on behalf of himself and all others similarly situated against Defendant Newport Harbor Pathology Medical Group, Inc. d/b/a Orange County Medical Group Pathology d/b/a Mission Laguna Pathology Medical Group d/b/a Barr Dermatopathology ("NHPMG" or "Defendant"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit on behalf of all California residents who are patients of Defendant and have received pathology and/or dermatopathology services provided by Defendant.

2. Plaintiff seeks to hold Defendant responsible for the injuries Defendant inflicted on Plaintiff and hundreds of similarly situated persons ("Class members") due to Defendant's impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized cybercriminals (the "Data Breach" or "Breach") between October 8, 2024, and November 11, 2024. The Breach was made public on January 10, 2025.[1]

JURISDICTION AND VENUE

3. The Court has personal jurisdiction over the matter because the events giving rise to the cause of action occurred as a result of Defendant's purposely directed contacts with California and its residents.

4. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs,

[1] US DEP'T OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 7, 2025).

there are more than 100 members in the proposed classes, and at least one Class Member, is a citizen of a state different from Defendant.

5. Venue is proper in this District under 28 U.S.C. §1391(b) because a substantial portion of the events giving rise to Plaintiff's claims occurred here.

THE PARTIES

Defendant

6. Defendant Newport Harbor Pathology Medical Group, Inc. d/b/a/ Orange County Medical Group Pathology d/b/a Mission Laguna Pathology Medical Group d/b/a Barr Dermatopathology ("NHPMG") is a California corporation with its principal place of business located at 2901 W. Coast Hwy, Suite 200, Newport Beach, CA 92663. Defendant owns and operates a group of pathologists servicing physician practices as well as hospital inpatients and outpatients in California.

Plaintiff

7. Plaintiff Matthew Miller is an adult citizen of the state of California and is domiciled in Mission Viejo, California.

8. Plaintiff Miller is a patient of Defendant and received pathology and/or dermatopathology services from Defendant in or around April 2023.

9. Plaintiff first received notice of the Data Breach in or around March, 2025, when he received a notice letter in the mail indicating that unauthorized actors may have accessed his personally identifiable information.

FACTUAL ALLEGATIONS

10. Defendant is a medical group operating a pathology practice throughout California. Defendant's "expanded group of 30 pathologists" provide a variety of pathology specialties. Specialties include but are not limited to "[b]reast pathology[,]" "[d]ermatopathology[,]" "[h]ematopathology[,]" and "[g]astrointestinal [p]athology[.]"[2]

[2] LAGUNA PATHOLOGY [NHPMG], ABOUT US, https://lagunapathology.com/.

11. As a condition of receiving its products and/or services, Defendant requires patients, including Plaintiff and Class members, to entrust it with highly sensitive personal information, including individuals' name, address, date of birth, driver's license or state ID number, and Social Security number ("personally identifiable information" or "PII"). Defendant retains this information for at least many years and even after the patient relationship has ended.

12. Defendant made promises and representations to its consumers, including Plaintiff and Class members, that the PII collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

13. Indeed, Defendant's Privacy Policy provides that it is Defendant's "policy to maintain reasonable and feasible physical, electronic and process safeguards to restrict unauthorized access to and protect the availability and integrity of your health information."

14. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would keep their sensitive PII confidential, maintain its system security, use the PII for business purposes only, and to only disclose the information to authorized and trusted personnel.

15. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumers' PII safe and confidential.

16. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

17. Defendant derived a substantial economic benefit from collecting

Plaintiff's and Class members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

18. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

A. The Data Breach

19. For over a month, Defendant NHPMG was unaware that its systems were compromised and that an unauthorized actor may have accessed patients' personally identifiable information.[3]

20. On November 11, 2024, Defendant first became "aware of unauthorized activity within a portion of [Defendant's] environment."[4] This unauthorized activity had been ongoing since at least October 8, 2024.[5]

21. Defendant goes on to explain that an "unauthorized actor potentially viewed and copied certain personal information stored within NHPMG's systems[.]"[6]

22. On January 10, 2025, NHPMG reported to the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") that NHPMG had experienced a "hacking/IT [i]ncident" and that the location of breached information was "[n]etwork [s]erver[.]"[7]

23. To date, Defendant's investigation has revealed that the "types of information that may be impacted include: name, Social Security number, date of

[3] *See* NHPMG, DATA BREACH NOTICE, https://lagunapathology.com/data-breach-notice/ (last accessed Apr. 7, 2025).

[4] NHPMG, DATA BREACH NOTICE, https://lagunapathology.com/data-breach-notice/ (last accessed Apr. 7, 2025).

[5] *See id.*

[6] *Id.*

[7] U.S. DEP'T OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 7, 2025).

birth, address, diagnosis, pathology test results (diagnosis), medical record number, driver's license numbers, unique or other government-issued identification numbers and health insurance information."[8]

24. Defendant concedes that it does not know the full extent of the Data Breach. For example, Defendant does not know "the exact information affected and to whom the information relates."[9]

B. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Valuable PII.

25. Defendant collected, retained, and stored the PII of Plaintiff and Class members and derived a substantial economic benefit from that PII. But for the collection of Plaintiff's and Class members' PII, Defendant would not be unable to perform its services.

26. Individuals, including Plaintiff and Class members, who are patients of Defendants and received pathology and/or dermatopathology services, were required to entrust Defendant with sensitive, non-public PII, to obtain services from Defendant. Defendant retains this information for at least many years, even after the patient relationship has ended.

27. By obtaining, collecting, and storing the PII of Plaintiff and Class members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

28. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[10]

---

[8] DATA BREACH NOTICE, NHPMG, https://lagunapathology.com/data-breach-notice/ (last accessed Apr. 7, 2025).

[9] *Id.*

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS, Oct. 16, 2019,

29. Driver's license numbers, which were likely compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[11] A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1,200 on the dark web. On its own, a forged license can sell for around $200.[12]

30. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[13] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[14]

31. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[15]

32. Based on the foregoing, the information at issue in the Data Breach is

---

https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 25, 2023).

[11] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, FORBES, Apr. 20, 2021, available at: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole- customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited Sept. 25, 2023).

[12] *Id*.

[13] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/

[14] *Id*.

[15] *How Identity Thieves Took My Wife for a Ride*, NY TIMES, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Sept. 21, 2023).

significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

33. Moreover, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud.[16]

34. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

35. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

36. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class members.

C. Defendant Knew Or Should Have Known It Was At Risk Of Cyberattacks

37. Defendant was aware or should have been aware of its vulnerabilities to cyberattacks like the one alleged.

38. Data thieves regularly target companies like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by sophisticated criminal parties who seek to illegally monetize that PII through unauthorized access.

39. According to the Identity Theft Resource Center's 2022 Data Breach

[16] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 25, 2023).

Report, 1,802 data compromises were reported in 2022, with 422.1 million people affected by the reported breaches.[17]

40. Healthcare data breaches are particularly common. Indeed, health care data breach statistics "clearly show there has been an upward trend in data breaches over the past 14 years[.]"[18]

41. According to the HIPAA Journal, "the leading provider of news, updates, and independent advice for HIPAA compliance[,]" "[d]ata breaches increased once again in 2022, with OCR receiving reports of 720 data breaches of 500 or more records."[19]

42. Pathology service providers are among the myriad of high profile health care data breaches.

43. For example, Clinical Pathology Laboratories, Inc. ("Clinical Pathology") reported a "[h]acking/IT [i]ncident" to OCR in 2019.[20]

44. Additionally, Associated Pathologists, LLC d/b/a PathGroup Health Plan ("Associated Pathologists") reported a "[h]acking/IT [i]ncident" to OCR in 2023.[21] Just like Defendant, Associated Pathologists indicated the "[l]ocation of [b]reached [i]nformation" was a "[n]etwork [s]erver[.]"[22]

45. In light of the myriad recent high profile data breaches at other health care companies, including Clinical Pathology and Associated Pathologists, Defendant

---

[17] https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/.

[18] Steve Alder, *Healthcare Data Breach Statistics*, THE HIPAA JOURNAL (Mar. 20, 2025) https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Apr. 7, 2025).

[19] *Id.*

[20] *Id.*

[21] U.S. DEP'T OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Apr. 7, 2025).

[22] *Id.*

knew or should have known that the PII they collected and maintained could and would be targeted by cybercriminals.

46. Despite this, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, allowing the attackers free access to the PII stored therein. Defendant failed to implement reasonable security procedures, failed to properly verify the credentials of the attacker, and failed to have in place systems to prevent and detect the unauthorized activity.

47. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

48. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to, upon information and belief, potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

49. Upon information and belief, Plaintiff's and Class members' unencrypted PII was compromised and stolen by the cyberattackers in the October 8, 2024 to November 11, 2024 Data Breach. Plaintiff further believes his PII, and that of Class members, has been or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

50. Defendant could have prevented the Data Breach by implementing reasonable security procedures and practices, properly securing its network and encrypting the files and files servers containing the PII of Plaintiff and Class members, and by taking the necessary steps to prevent breaches from occurring after similar health care data breach incidents.

51. Once it was made aware of the Data Breach, Defendant did not take any immediate action to alert Plaintiff and Class members of the Breach, nor did it take reasonable steps in ensuring the PII would not be further compromised or made public. In fact, Defendant has yet to disclose **any** information regarding the specific details of the Data Breach to those injured, including Plaintiff and Class members.

52. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

D. Defendant Failed To Comply With FTC Guidelines

53. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an 'unfair practice' in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

54. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

58. Defendant was at all times fully aware of its obligation to protect the PII of its consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed To Comply With Industry Standards

59. Despite its alleged commitment to securing sensitive PII, Defendant does not follow industry standard practices in securing PII.

60. Some industry best practices that should be implemented by entertainment companies dealing with sensitive PII, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access

sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

61. Other best cybersecurity practices that are standard in the entertainment industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

62. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC- 1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. Defendant failed to comply with these accepted standards in the entertainment industry, thereby permitting the Data Breach to occur.

F. Common Injuries and Experiences of Plaintiff and Class Members

64. Plaintiff and Class members are California residents who have received pathology and/or dermatopathology services from Defendant. In doing so, Plaintiff and Class members were required to provide their PII to Defendant, including but not limited to, name, date of birth, contact information, and Social Security number.

65. At the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

66. Plaintiff is very careful about sharing his sensitive PII. Plaintiff regularly monitors his credit and banking information and has increased his monitoring since learning of the breach. Plaintiff plans on changing his relevant passwords and pins since learning of the breach.

67. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

68. When Defendant announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. To date, Defendant has failed to explain how the Breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

69. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class members, including but not limited to, their PII ending up in the possession of criminals, the risk of identity theft, invasion of privacy, the continued mitigation of the materialized risk of identity theft, and the loss of benefit of the bargain.

70. Plaintiff and Class members entrusted their PII to Defendant and were deprived of the benefit of their bargain. Plaintiff had the reasonable expectation and understanding that Defendant would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted his PII to any entity that used Defendant's services had they known that Defendant would not take reasonable steps to safeguard their information. Accordingly, Plaintiff and Class members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

71. The unencrypted PII of Plaintiff and Class members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class members. Unauthorized individuals can easily access the PII of Plaintiff and Class members.

72. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes.

73. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes——e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

74. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

75. Consequently, Plaintiff and Class members are at a present and continuous risk of fraud and identity theft for many years into the future.

76. Plaintiff and Class members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

77. As a result of the Data Breach, Plaintiff and Class members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class members

will suffer anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

78. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

79. Plaintiff and Class members have a continuing interest in ensuring that their PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

80. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

81. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ALLEGATIONS

82. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

83. Plaintiff seeks to represent a class defined as "All Individuals whose PII was disclosed in the Data Breach (the "Class").

84. Plaintiff also seek to represent a subclass defined as "All California residents whose PII was disclosed in the Data Breach" (the "California Subclass")

85. Excluded from the Class are Defendant and its parents or subsidiaries,

any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

86. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

87. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

88. Numerosity. The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes potentially hundreds of thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

89. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant's response to the Data Breach was adequate;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class members' PII;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and

regulations;

h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendant owed a duty to Class members to safeguard their PII;

j. Whether Defendant breached its duty to Class members to safeguard their PII;

k. Whether hackers obtained Class members' PII via the Data Breach;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

90. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class members

because, inter alia, all Class members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class members arise from the same operative facts and are based on the same legal theories.

91. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

92. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class members in that all of Plaintiff's and Class members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

93. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

94. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

95. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class members affected by the Data Breach.

COUNT I
Negligence and Negligence *Per Se*
(On behalf of Plaintiff and the Class)

96. Plaintiff restates and realleges each and every paragraph above as if fully set forth herein.

97. Defendant requires its consumers, including Plaintiff and Class members, to submit non-public PII in the ordinary course of providing its services.

98. Defendant gathered and stored the PII of Plaintiff and Class members as part of its business of soliciting its services to its consumers, which solicitations and services affect commerce.

99. Plaintiff and Class members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

100. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members could and would suffer if the PII were wrongfully disclosed.

101. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

102. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or

affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

103. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

104. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being consumers of Defendant.

105. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

106. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

107. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former consumers' PII it was no longer required to retain pursuant to regulations.

108. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

109. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

110. Defendant breached its duties, pursuant to the FTCA and other applicable

standards, and thus was negligent, by failing to use reasonable measures to protect Class members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class members' PII;

e. Failing to detect in a timely manner that Class members' PII had been compromised;

f. Failing to remove former consumers' PII it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

111. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

112. Plaintiff and Class members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm it was intended to guard against.

113. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

114. The FTC has pursued enforcement actions against businesses, which, as

a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

115. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

116. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the entertainment industry.

117. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

118. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

119. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

120. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

121. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

122. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a

special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

123. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

124. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiffs and the Class would not have been compromised.

125. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other

economic and non-economic losses.

128. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

129. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

130. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class members in an unsafe and insecure manner.

131. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

132. Plaintiff restates and realleges each and every paragraph above as fully set forth herein.

133. Plaintiff and Class members were required to provide their PII to Defendant as a condition of receiving services and loyalty program membership from Defendant.

134. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

135. In entering into such implied contracts, Plaintiff and Class members

reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

136. Implicit in the agreement between Plaintiff and Class members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

137. The mutual understanding and intent of Plaintiff and Class members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

138. Defendant solicited, offered, and invited Plaintiff and Class members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their PII to Defendant.

139. In accepting the PII of Plaintiff and Class members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

140. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

141. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class members' PII would remain protected.

142. Plaintiff and Class members paid money and provided their PII to Defendant with the reasonable belief and expectation that Defendant would use part

of its earnings to obtain adequate data security. Defendant failed to do so.

143. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

144. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

145. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

146. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

147. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

148. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

149. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT III
Restitution or Unjust Enrichment
(On Behalf of Plaintiff and the Class)

150. Plaintiff restates and realleges each and every paragraphs above as if fully set forth herein.

151. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count II).

152. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they paid for services from and enrolled in loyalty program membership with Defendant and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

153. Defendant knew that Plaintiff and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business purposes.

154. Defendant failed to secure Plaintiff's and Class members' PII and, therefore, did not fully compensate Plaintiff or Class members for the value that their PII provided.

155. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

156. If Plaintiff and Class members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII at Defendant or obtained loyalty program membership at Defendant.

157. Plaintiff and Class members have no adequate remedy at law.

158. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon it.

159. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

160. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class members may seek restitution or compensation.

161. Plaintiff has no adequate remedy at law for this claim. Plaintiff pleads his claim for unjust enrichment in the alternative, which inherently would necessitate a finding of no adequate remedy at law. Alternatively, legal remedies available to Plaintiff is inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also U.S. v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. Oct. 6, 1992) ("the 'mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief"); *Quist v. Empire Water Co.*, 2014 Cal. 646, 643 (1928) ("The mere fact that there may be a remedy at law does not oust the jurisdiction of a court of equity. To have this effect, the remedy must also be speedy, adequate, and efficacious to the end in view … It must reach the whole mischief and secure the whole right of the party in a perfect manner at the present time and not in the future"). Furthermore:

a. To the extent damages are available here, damages are not equally certain as restitution because the standard that governs ordering restitution is different than the standard that governs damages.

Hence, the Court may award restitution even if it determines that Plaintiff fails to sufficiently adduce evidence to support an award of damages.

b. Damages and restitution are not necessarily the same amount. Unlike damages, restitution is not limited to the amount of money defendant wrongfully acquired plus the legal rate of interest. Equitable relief, including restitution, entitles Plaintiff to recover all profits from the wrongdoing, even where the original funds taken have grown far greater than the legal rate of interest would recognize. Plaintiff seeks such relief here.

c. Legal claims for damages are not equally certain as restitution because claims under the UCL and unjust enrichment entail few elements.

162. A claimant otherwise entitled to a remedy for unjust enrichment, including a remedy originating in equity, need not demonstrate the inadequacy of available remedies at law." Restatement (Third) of Restitution, § 4(2).

COUNT IV
California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

163. Plaintiff restates and realleges each and every paragraphs above as if fully set forth herein.

164. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

165. NHPGM is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code § 1798.81.5, of Plaintiff and Class members.

166. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

167. NHPMG is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

168. Plaintiff's and Class members' PII (*e.g.*, Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

169. Because NHPMG reasonably believed that Plaintiff's and Class members' PII was acquired by unauthorized persons during the NHPMG Data Breach, NHPMG had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

170. NHPMG failed to fully disclose material information about the Data Breach, including the types of PII impacted.

171. By failing to disclose the Data Breach in a timely and accurate manner, NHPMG violated Cal. Civ. Code § 1798.82.

172. As a direct and proximate result of NHPMG's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and Class members suffered damages, as described above.

173. Plaintiff and Class members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT V
California Unfair Competition Act
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

174. Plaintiff restates and realleges each and every paragraphs above as if fully set forth herein.

175. NHPMG is a "person" as defined by Cal. Bus. & Prof. Code §17201.

176. NHPMG violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

177. NHPMG's "unfair" acts and practices include:

a. NHPMG failed to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. NHPMG failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and Class members, whose PII has been compromised.

c. NHPMG's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. NHPMG's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described

above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of NHPMG's grossly inadequate security, consumers could not have reasonably avoided the harms that NHPMG caused.

e. NHPMG engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

178. NHPMG has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

179. NHPMG's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class member's members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and

Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*. and 1798.81.5, which was a direct and proximate cause of the Data Breach.

180. NHPMG's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NHPMG's data security and ability to protect the confidentiality of consumers' PII.

181. As a direct and proximate result of NHPMG's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for NHPMG's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

182. NHPMG acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class members rights. Myriad high profile health care data breaches—including pathology service providers—put NHPMG that its security and privacy protections were

inadequate.

183. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from NHPMG's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. For a determination that this action is a proper class action;

b. For an order certifying the Classes, naming Plaintiff as representative of the Classes, and naming Plaintiff's attorneys as Class Counsel to represent the Classes;

c. For an order declaring that Defendant's conduct violated the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

e. For an award of compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. For punitive damages, as warranted, in an amount to be determined at trial;

g. For an injunctive requiring Defendant to adequately safeguard the PII of Plaintiff and the Classes by implementing security procedures, included but not limited to:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption,

all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class members' PII;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portion's of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security

training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

h. For prejudgment interest on all amounts awarded;

i. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit; and

j. For an order granting Plaintiff and Class members such further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Classes, demands` a trial by

jury for all of the claims asserted in this Complaint so triable.

Dated: April 7, 2025

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*

Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646)-837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

Attorney for Plaintiff